

JOSEPH H. HUNT
Assistant Attorney General
DAVID L. ANDERSON
United States Attorney
ANTHONY J. COPPOLINO
Deputy Branch Director
JULIA A. HEIMAN
Senior Counsel
CHRISTOPHER HEALY
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch

P.O. Box 883
Washington, D.C. 20044
Telephone: (202) 616-8480
Facsimile: (202) 616-8470
Email: julia.heiman@usdoj.gov

Attorneys for Defendants

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

TWITTER, INC.,

Plaintiff,

v.

WILLIAM P. BARR, Attorney
General of the United States, *et al.*,

Defendants.

Case No. 14-cv-4480-YGR

**DEFENDANTS' REQUEST
THAT THE COURT
DISCHARGE THE ORDER TO
SHOW CAUSE AND DENY
PLAINTIFF'S REQUEST FOR
ACCESS TO THE CLASSIFIED
STEINBACH DECLARATION,
OR, IN THE ALTERNATIVE,
MOTION TO DISMISS IN
LIGHT OF THE ATTORNEY
GENERAL'S ASSERTION OF
THE STATE SECRETS
PRIVILEGE**

Hon. Yvonne Gonzalez Rogers

Twitter, Inc. v. Barr, et al., Case No. 14-cv-4480-YGR
Defs.' Req. that the Court Discharge the Order to Show Cause and
Deny Pl.'s Req. for Access to the Classified Steinbach Decl., or in the Alternative,
Motion to Dismiss in Light of the Attorney General's Assertion of the State Secrets Privilege

1 **NOTICE OF MOTION**

2 For the reasons set forth in Defendants' accompanying Memorandum of Points and
3 Authorities, Defendants respectfully request that the Court discharge the Order to Show Cause,
4 *see* ECF No. 261, and deny Plaintiff's request for access to the Classified Steinbach Declaration.

5 PLEASE TAKE NOTICE that, in the alternative, Defendants seek dismissal of the
6 Plaintiff's Second Amended Complaint for the reasons set forth in Defendants' accompanying
7 Memorandum of Points and Authorities. Consistent with the Court's February 14, 2019, Order
8 that directs the parties to submit jointly a schedule for further proceedings based on the
9 Government's decision regarding an assertion of the state secrets privilege, *see* ECF No. 272, the
10 Defendants will confer with Plaintiff and intend, on March 19, 2019, to submit a proposed
11 schedule for further briefing and oral argument on this motion.

12
13 Dated: March 15, 2019

Respectfully submitted,

14
15 JOSEPH H. HUNT
16 Assistant Attorney General

17 DAVID L. ANDERSON
18 United States Attorney

19 ANTHONY J. COPPOLINO
20 Deputy Branch Director

21 /s/ Julia A. Heiman
22 JULIA A. HEIMAN, Bar No. 241415
23 Senior Counsel
24 CHRISTOPHER HEALY
25 Trial Attorney
26 U.S. Department of Justice
27 Civil Division, Federal Programs Branch
28 P.O. Box 883
Washington, D.C. 20044
julia.heiman@usdoj.gov
Attorneys for Defendants

TABLE OF CONTENTS

| | | |
|------|--|----|
| I. | INTRODUCTION..... | 1 |
| II. | BACKGROUND | 5 |
| III. | CATEGORIES OF INFORMATION SUBJECT TO THE ATTORNEY GENERAL’S ASSERTION OF PRIVILEGE..... | 10 |
| IV. | ARGUMENT..... | 10 |
| A. | The Attorney General has Properly Invoked the State Secrets Privilege to Protect the Sensitive National Security Information in the Classified Steinbach Declaration..... | 12 |
| 1. | Disclosure of the Information at Issue Reasonably Could Be Expected to Result in Significant Harm to the National Security..... | 14 |
| 2. | Disclosure to Cleared Counsel Would Create the Risks of Harm Discussed Herein..... | 17 |
| 3. | The States Secrets Privilege Has Been Asserted Only to the Extent Necessary in this Matter..... | 21 |
| 4. | The Proper Invocation of Privilege Over These Categories of Information Renders Them Unavailable for Any Purpose in this Litigation. | 22 |
| B. | Because this Case Cannot Be Litigated Without the Privileged Evidence, Binding Precedent Requires that Plaintiff’s Claims Be Dismissed..... | 23 |
| V. | CONCLUSION..... | 25 |

TABLE OF AUTHORITIES

Cases

| | |
|---|---------------|
| <i>Admiral Ins. Co. v. U.S. Dist. Court for Dist. of Ariz.</i> , 881 F.2d 1486 (9th Cir. 1989) | 22 |
| <i>Al-Haramain Islamic Found., Inc. v. Bush</i> , 507 F.3d 1190 (9th Cir. 2007) | <i>passim</i> |
| <i>Al-Haramain Islamic Found., Inc. v. U.S. Dep’t of Treasury</i> , 686 F.3d 965 (9th Cir. 2012) | 17 |
| <i>CIA v. Sims</i> , 471 U.S. 159 (1985)..... | 13 |
| <i>Dep’t of Navy v. Egan</i> , 484 U.S. 518 (1988)..... | 3, 18 |
| <i>Dorfmont v. Brown</i> , 913 F.2d 1399 (9th Cir. 1990) | 3, 18 |
| <i>El-Masri v. United States</i> , 479 F.3d 296 (4th Cir. 2007) | 17 |
| <i>Ellsberg v. Mitchell</i> , 709 F.2d 51 (D.C. Cir. 1983)..... | 17 |
| <i>Farnsworth Cannon, Inc. v. Grimes</i> , 635 F.2d 268 (4th Cir. 1980) | 25 |
| <i>Fitzgerald v. Penthouse Int’l Ltd.</i> , 776 F.2d 1236 (4th Cir. 1985) | 25 |
| <i>Halkin v. Helms</i> , 598 F.2d 1 (D.C. Cir. 1978)..... | 16, 17 |
| <i>Holder v. Humanitarian Law Project</i> , 561 U.S. 1 (2010)..... | 13 |
| <i>In re Copley Press, Inc.</i> , 518 F.3d 1022 (9th Cir. 2008) | 22 |
| <i>Kasza v. Browner</i> , 133 F.3d 1159 (9th Cir. 1998) | 4, 12, 23 |
| <i>Twitter, Inc. v. Barr, et al.</i> , Case No. 14-cv-4480-YGR Defs.’ Req. that the Court Discharge the Order to Show Cause and Deny Pl.’s Req. for Access to the Classified Steinbach Decl., or in the Alternative, Motion to Dismiss in Light of the Attorney General’s Assertion of the State Secrets Privilege | |

| | | |
|----|--|----------------|
| 1 | <i>Mohamed v. Jeppesen Dataplan, Inc.</i> , | |
| 2 | 614 F.3d 1070 (9th Cir. 2010) | <i>passim</i> |
| 3 | <i>Snepp v. United States</i> , | |
| 4 | 444 U.S. 507 (1980)..... | 1 |
| 5 | <i>Sterling v. Tenet</i> , | |
| 6 | 416 F.3d 338 (4th Cir. 2005) | 17 |
| 7 | <i>Stillman v. CIA</i> , | |
| 8 | 319 F.3d 546 (D.C. Cir. 2003)..... | <i>passim</i> |
| 9 | <i>Tilden v. Tenet</i> , | |
| 10 | 140 F. Supp. 2d 623 (E.D. Va. 2000) | 17 |
| 11 | <i>United States v. Reynolds</i> , | |
| 12 | 345 U.S. 1 (1953)..... | 10, 11, 12, 23 |
| 13 | <i>Wikimedia Found. v. NSA</i> , | |
| 14 | 2018 WL 3973016 (D. Md. Aug. 20, 2018) | 16 |
| 15 | Other Authorities | |
| 16 | Executive Order 13526, 75 Fed. Reg. 707 (Dec. 29, 2009)..... | 18 |

28 *Twitter, Inc. v. Barr, et al.*, Case No. 14-cv-4480-YGR
 Defs.’ Req. that the Court Discharge the Order to Show Cause and
 Deny Pl.’s Req. for Access to the Classified Steinbach Decl., or in the Alternative,
 Motion to Dismiss in Light of the Attorney General’s Assertion of the State Secrets Privilege

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

At the heart of this case is Plaintiff Twitter, Inc.’s challenge to the Government’s determination that Plaintiff may not lawfully publish certain information about the extent to which it has received national security legal process from the Government. *See* Second Am. Compl., ECF No. 114, *generally*. Multiple Original Classification Authorities have determined that the information Twitter seeks to publish is properly classified. *See* Sept. 9, 2014 Letter From J. Baker to M. Sussmann, ECF No. 1-1, at 1; Unclassified Decl. of Executive Assistant Director (“EAD”) Steinbach, ECF No. 147-1, ¶ 29; Aug. 28, 2017 Decl. of EAD Ghattas, ECF No. 179-1, ¶ 6; Unclassified Decl. of Acting EAD McGarrity, attached as Exhibit B hereto (“Unclassified McGarrity Decl.”), ¶¶ 19, 22. From the outset of this case, the Government has urged the Court to proceed as courts have done in an analogous body of case law in federal jurisprudence where a party subject to a nondisclosure obligation claims a First Amendment right to publish information it has received from the Government: by examining *ex parte, in camera* the Government’s classified explanation of the harm to national security that reasonably could be expected to result from the proposed disclosure. *See, e.g., Stillman v. CIA*, 319 F.3d 546 (D.C. Cir. 2003). This is an appropriate and sensible framework for resolving the key question at issue in this case: whether Plaintiff has a First Amendment right to publish information that the Government has determined is properly classified and the disclosure of which reasonably could be expected to cause serious damage to national security. *See Snepp v. United States*, 444 U.S. 507, 509-510 & n.3 (1980) (*per curiam*) (person subject to secrecy obligation has no First Amendment right to publish classified information). The resolution of that question should be straightforward: if the Government shows that the information at issue is properly classified, including by establishing the risk of harm to national security that reasonably could be expected to result from its disclosure, Plaintiff’s claims should be dismissed. At the outset of this case, in resolving a motion to dismiss, the Court initially appeared to agree that this was an appropriate framework for resolving this litigation. *See* ECF No. 113 at 8.

1 But at the summary judgment stage, the case shifted course dramatically, and that has led
2 to the present posture. Plaintiff insisted that its counsel be granted a security clearance for access
3 to classified information that might be at issue in resolving its claims. The Government made
4 clear its opposition to that request, and that issue was unresolved when the Court ordered the
5 Government to submit its summary judgment motion on the merits, including any classified
6 submission. The Government expressed concern about this manner of proceeding because the
7 classified explanation it would prepare for the Court to demonstrate that the information Twitter
8 sought to publish is classified would itself contain sensitive national security information that
9 was broader and more detailed than Plaintiff or its counsel would know or have reason to learn.
10 *See* Oct. 24, 2016 Tr., ECF No. 138, at 31:2–17. The Government also argued that litigation
11 regarding access to classified information in this case was neither necessary nor appropriate, and
12 could make resolution of the merits of Plaintiff’s claims difficult or impossible. *Id.* at 12:21–
13 13:8; 25:22–25; 27:8–14. Despite these warnings, and with the question of access by Plaintiff’s
14 counsel unresolved, the Court ordered the Government to provide its classified explanation on
15 summary judgment or be precluded from doing so later. *Id.* at 31:13–24; 32:4–13. To avoid
16 such preclusion, the Government submitted the Classified Declaration of FBI Executive
17 Assistant Director Steinbach, *see* Notice of Lodging of Classified Declaration, ECF No. 144
18 (“Classified Steinbach Declaration”) concurrently with its summary judgment motion to explain
19 why the information Twitter sought to publish is properly classified, including why disclosure of
20 the information reasonably could be expected to result in serious damage to national security.

21 After the Court denied without prejudice the Government’s summary judgment motion, it
22 granted Plaintiff’s motion to initiate a background investigation of its counsel. Plaintiff then
23 began to seek access to the Classified Steinbach Declaration. Plaintiff served discovery requests
24 which called for the document and other classified information, and made its first formal request
25 of the Court to compel access to the classified declaration on November 26, 2018, after
26 Plaintiff’s counsel’s background investigation to determine his suitability for access to classified
27 information had been favorably adjudicated. The Court then issued an Order to Show Cause
28

1 why the Government should not be compelled to disclose the Classified Steinbach Declaration to
2 Plaintiff's counsel. *See* ECF No. 261.

3 In response to the Plaintiff's request and the Order to Show Cause, the Government filed
4 multiple submissions urging the Court to deny the Plaintiff's request, both based on the
5 Executive's constitutional authority to protect and control access to classified information, *see*
6 *Dep't of Navy v. Egan*, 484 U.S. 518, 527 (1988); *Dorfmont v. Brown*, 913 F.2d 1399, 1401 (9th
7 Cir. 1990), and because Plaintiff's demand to compel disclosure would trigger consideration of
8 an assertion of the state secrets privilege if necessary to protect the Classified Steinbach
9 Declaration from disclosure – a step which the Government explained could render impossible
10 the resolution of the merits of Plaintiff's First Amendment claims. *See* ECF Nos. 256, 264, 269.

11 Because the Plaintiff's demand for access and the Order to Show Cause remain pending,
12 the Government has proceeded with its consideration of an assertion of the state secrets
13 privilege, and as set forth herein, the Attorney General of the United States has now asserted that
14 privilege to protect the Classified Steinbach Declaration from disclosure to Plaintiff's counsel.
15 This case is thus now in an extraordinary posture: the Court previously ordered the Government
16 to submit its summary judgment motion and accompanying classified explanation to the Court
17 before the question of access by Plaintiff's counsel was resolved, and then issued an order to
18 show cause why that detailed explanation, submitted solely for the court's *ex parte, in camera*
19 consideration, should not be disclosed—over the Government's objection—to counsel for a
20 private party in a civil suit. The Government has previously urged the Court to obviate the need
21 for an assertion of the state secrets privilege by denying the Plaintiff's request for access to
22 classified information and discharging the Order to Show Cause on other grounds, *see* ECF Nos.
23 264, 269, and permitting litigation regarding the merits of Plaintiff's claims to move forward.
24 Should the Court do so, there would be no need to address either the assertion of the state secrets
25 privilege discussed herein or the need to dismiss Plaintiff's claims on that basis, which, as
26 explained below, would necessarily follow if the privilege is upheld.

27 But to the extent the Court may still order the disclosure of the Classified Steinbach
28 Declaration to Plaintiff's counsel, the Attorney General has now asserted privilege over that
Twitter, Inc. v. Barr, et al., Case No. 14-cv-4480-YGR
3
Defs.' Req. that the Court Discharge the Order to Show Cause and
Deny Pl.'s Req. for Access to the Classified Steinbach Decl., or in the Alternative,
Motion to Dismiss in Light of the Attorney General's Assertion of the State Secrets Privilege

document. *See* Decl. of William P. Barr, the Attorney General of the United States, attached as Ex. A hereto (“AG Decl.”). As explained below, the Classified Steinbach Declaration, in explaining why the information Twitter seeks to publish is properly classified, contains four categories of classified information. After personal consideration of the matter, the Attorney General has determined that disclosure of that information, even to Plaintiff’s counsel, reasonably could be expected to cause significant harm to the national security. *See* AG Decl. ¶¶ 3–14. In support of the Attorney General’s privilege assertion, the Government also submits herewith the Unclassified Declaration of the Acting Executive Assistant Director of the Federal Bureau of Investigation Michael C. McGarrity, attached as Exhibit B hereto, as well as the Classified Declaration of Acting EAD McGarrity, lodged with the Court Information Security Officer solely for the Court’s *ex parte*, *in camera* review. Both declarations by Acting EAD McGarrity explain further the grounds for the Attorney General’s assertion of privilege.

When the Government asserts the state secrets privilege to protect information from disclosure, a court must undertake a three-step analysis. *See Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070 (9th Cir. 2010). In the first and second steps, a court must determine whether the privilege has been properly invoked as a procedural and substantive matter. *See id.* Here, as explained below, both of these requirements are fulfilled. The Attorney General, as head of the Department of Justice, has formally asserted the privilege and has determined that disclosure of the privileged information, including to Plaintiff’s counsel, reasonably could be expected to cause significant harm to national security. *See* AG Decl. ¶ 13; *see also* Unclassified McGarrity Decl. 33–40. As a result, if the privilege is upheld, the privileged information would be “completely removed from the case.” *Jeppesen*, 614 F.3d at 1082 (quoting *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998)). As the third and final step of the analysis, where a court finds that privilege has properly been invoked, it then must assess “whether the action can be litigated without relying on evidence that would necessarily reveal [state] secrets or press so closely upon them as to create an unjustifiable risk that they would be revealed.” *Id.* at 1085.

Here, the Attorney General has asserted privilege over four categories of information in the Classified Steinbach Declaration, including not only the classified information that Twitter *Twitter, Inc. v. Barr, et al.*, Case No. 14-cv-4480-YGR
4
Defs.’ Req. that the Court Discharge the Order to Show Cause and
Deny Pl.’s Req. for Access to the Classified Steinbach Decl., or in the Alternative,
Motion to Dismiss in Light of the Attorney General’s Assertion of the State Secrets Privilege

initially sought to publish, but also, a detailed explanation of the harms that reasonably could be expected to result from disclosure of that information, including a description of the ways in which adversaries of the United States would be able to use that information to the detriment of the national security of the United States. *See* AG Decl. ¶¶ 4, 6–9. Thus, the Classified Steinbach Declaration, over which privilege has now been asserted, stands at the very center of this litigation, for it is central to explaining why Twitter has no First Amendment right to publish information that would harm national security. “There is no feasible way to litigate [the Government’s] alleged liability without” this information or without “creating an unjustifiable risk of divulging state secrets.” *Jeppesen*, 614 F.3d at 1087. Indeed, in such a circumstance, as explained below, “any plausible effort” by the Government to address Plaintiff’s claims would depend upon, and place at risk, the privileged information at issue. *Id.*

For all these reasons, as discussed herein and in Defendants’ recent submissions, the Court should deny the Plaintiff’s request for access to the Classified Steinbach Declaration and discharge the Order to Show Cause. Indeed, the Court may do so without reaching the Attorney General’s assertion of privilege for reasons previously set forth by the Defendants.¹ However, if the Court is still considering whether to grant Plaintiff’s counsel access to the Classified Steinbach Declaration, it should uphold the Attorney General’s state secrets privilege assertion over the classified information in that document, exclude that information from the litigation, and dismiss the Second Amended Complaint on that basis.

II. BACKGROUND

Plaintiff filed the currently-operative complaint in May 2016, challenging, *inter alia*, whether the information that it sought to publish was properly classified. *See* Second Am. Compl., ECF No. 114. Defendants responded by seeking a conference to set a schedule for summary judgment briefing, urging the Court to resolve this case using the procedures set forth in *Stillman v. CIA*, which provides that in cases challenging classification determinations by

¹ As explained in the Government’s prior submissions, such an order would be contrary to law, since the Constitution vests the protection and control of classified information in the Executive Branch. *See* ECF Nos. 256, 264, 269 (discussing case law).

persons subject to nondisclosure obligations, “*in camera* review of affidavits, followed if necessary by further judicial inquiry, will be the norm.” *See* ECF No. 116 at 2 (quoting *Stillman*, 319 F.3d at 548–49). The Court denied the Defendants’ request, and indicated that a responsive pleading would be required prior to summary judgment briefing. *See* ECF No. 119. Defendants submitted their answer to the Second Amended Complaint on July 5, 2016. *See* Answer, ECF No. 120.

On September 21, 2016, Plaintiff submitted its Motion for an Order Directing Defendants to Initiate an Expedited Security Clearance Process for Plaintiff’s Counsel, ECF No. 124. Defendants opposed that motion, explaining that this case should be resolved, as in *Stillman v. CIA*, based on the Court’s *ex parte, in camera* review of the Government’s submission of a classified explanation of why the information that Plaintiff seeks to publish is properly classified. *See* ECF No. 133 at 4–8. Defendants also explained that there is no support in the case law for granting counsel access to classified information in this setting. *See id.* at 8–12. Moreover, Defendants noted that an order granting Plaintiff’s request for background investigations would “risk[] sidetracking the case into potentially complex litigation over access to classified information,” and, in particular that such an order “[would] set the stage for potential disputes over the denial of access by the Government for purposes of this case, or for assertions of privilege in response to discovery demands for classified information.” *See id.* at 12 & n.7.

At a subsequent case management conference, on October 24, 2016, counsel for the Defendants reiterated that this case should move forward pursuant to the procedure established by *Stillman* and its progeny, and avoid the difficult issues that would arise if Plaintiff were to request access to classified information. *See* Oct. 24, 2016 Tr., ECF No. 138, 5:2 –6:20; *id.* 14:5–14; *id.* 20:1–16; *id.* 28:19–29:10. Counsel further explained that, in this case, the heart of the matter—the Government’s explanation of why publication of the information in Twitter’s draft Transparency Report reasonably could be expected to harm national security—would itself be classified. In such circumstances, counsel explained that courts do not typically permit discovery, because a request for access to such information could result in “the Government [having] to consider whether to assert the state secrets privilege with . . . potentially serious

1 consequences for the litigation.” *Id.* at 25:22–25; *see also id.* 12:21–13:8 (explaining that a
2 request for access to classified information “would raise questions about whether the case could
3 be litigated on the merits at all”); *id.* 27: 8–14.

4 At the same status conference, because Defendants had emphasized that whether
5 discovery should be permitted at all was inextricably intertwined with the more global question
6 of how the case should proceed, the Court instructed Defendants to submit their summary
7 judgment motion. *Id.* at 30:14–22. Counsel raised concerns about submitting a classified
8 declaration supporting a summary judgment motion at a time when Plaintiff’s motion for a
9 background investigation was pending, explaining that what the Government could present to the
10 Court *ex parte* would be more fulsome and detailed than anything that could be shared with
11 Plaintiff’s counsel. *See id.* at 31:2–17. The Court nonetheless ordered the Government to
12 proceed, including with its *ex parte* presentation, noting that, otherwise, the Government would
13 later be precluded from making such a motion. *See id.* at 31:13–24; 32:4–13.

14 Consistent with the Court’s Order, Defendants submitted their motion for summary
15 judgment, *see* ECF No. 145, including the Classified Steinbach Declaration, explaining why
16 publication of the information in Plaintiff’s draft Transparency Report reasonably could be
17 expected to harm national security. *See* Notice of Lodging of Classified Declaration, ECF No.
18 144. Defendants also submitted an unclassified version of that declaration, providing as much
19 information from EAD Steinbach’s classified declaration as possible, consistent with the national
20 security, on the public record. *See* Unclassified Declaration of EAD Steinbach, ECF No. 147-1,
21 ¶ 1. In his unclassified declaration, EAD Steinbach noted his understanding that the classified
22 declaration would be made available to the Court “solely for its *ex parte* and *in camera* review.”
23 *Id.* at 1 n.1. He further emphasized that “[f]or the reasons explained in the classified declaration,
24 disclosure of the information contained therein reasonably could be expected to result in damage
25 to the national security.” *Id.* On July 6, 2017, the Court denied without prejudice the
26
27
28

Government’s summary judgment motion, and granted Plaintiff’s motion that the Government be ordered to initiate a background investigation of its counsel. *See* ECF No. 172.²

While the Defendants’ summary judgment motion had been pending, Plaintiff served its discovery requests and Defendants responded with their objections; although Plaintiff’s requests called for classified and unclassified responses, including the Classified Steinbach Declaration, the parties’ February 17, 2017 joint letter brief made clear that Plaintiff was not seeking to compel access to classified information at that time. *See* Joint Letter Brief, ECF No. 167 at 1 n.2 (“Twitter’s discovery requests include requests for unclassified as well as classified information . . . but Twitter seeks at this time to compel only unclassified discovery.”). On August 8, 2017, Defendants submitted a declaration from EAD Carl Ghattas, who became Executive Assistant Director of FBI’s National Security Branch after EAD Steinbach retired, describing the requirements that must be fulfilled before any individual may access classified information. *See* Aug. 8, 2017 Ghattas Decl., ECF No. 175-1, ¶¶ 9–16. EAD Ghattas attested that the FBI had determined that Plaintiff’s counsel do not fulfill those requirements with respect to the classified information at issue in this case—including the Classified Steinbach Declaration—because the FBI has determined that counsel lack a “need-to-know” that information, as defined by the operative Executive Order. *See id.*, ¶¶ 17–21; *see also infra* at 18.³

On February 12, 2018, the Court overruled a number of Defendants’ objections to Plaintiff’s discovery requests, *see* ECF No. 188, and the parties have proceeded with discovery, in which Defendants have provided logs for classified materials and produced materials from unclassified systems, as well as related privilege logs, as summarized in the parties’ recent updated case management statement. *See* Fourth Updated Joint Case Management Statement,

² Consistent with the Court’s Order, the Government completed a background investigation of Plaintiff’s counsel. That background investigation was favorably adjudicated. *See* Fourth Updated Joint Case Management Statement, ECF No. 244 at 7. As explained herein, this step does not constitute a grant of access by the Executive Branch to any particular classified information.

³ On August 28, 2017, Defendants submitted a declaration from EAD Ghattas stating that he had reviewed the classified and unclassified declarations of EAD Steinbach, and concurred with the conclusions therein. *See* ECF No. 179-1, ¶¶ 5–6.

ECF No. 244 at 10–13. Defendants have reviewed for responsiveness and logged classified materials, including the Classified Steinbach Declaration. Plaintiff has not, to date, moved to compel disclosure of other classified materials. But at the November 26, 2018 case management conference, Plaintiff specifically requested access to the Classified Steinbach Declaration that Defendants had submitted in support of their summary judgment motion. *See* Nov. 26, 2018 Tr., ECF No. 251, at 8:20–22, 13:2–5; *see also* Fourth Updated Joint Case Management Statement, ECF No. 244 at 7 (noting, on November 19, 2018, that “Twitter [then] intend[ed] to move the Court for an order granting Twitter’s cleared counsel access to Defendants’ classified submission). The Court ordered that Plaintiff submit a formal written request by December 5, 2018, Nov. 26, 2018 Tr., ECF No. 251, at 16: 23–24, and Plaintiff submitted such a request. *See* ECF No. 250. The Court further ordered that, in a December 17, 2018, submission, Defendants inform the Court, *inter alia*, whether they intend to consider an assertion of the state secrets privilege in response to Plaintiff’s request for access to the Classified Steinbach Declaration. Tr., ECF No. 251, at 23:20–24:5. On December 17, 2018, Defendants stated that they had initiated the process of considering whether to assert the state secrets privilege, but asked the Court to deny the Plaintiff’s request for access on other grounds. *See* ECF No. 256.

On January 2, 2019, the Court entered the Order to Show Cause re: Disclosure of Declaration Submitted in Camera, ordering Defendants to show cause why they should not be compelled to disclose the Classified Steinbach Declaration to Plaintiff’s Counsel. *See* ECF No. 261 (“Order to Show Cause”). In briefing submitted in response to the Order to Show Cause, Defendants noted that they were continuing to consider an assertion of the state secrets privilege to protect the classified information in the Classified Steinbach Declaration, but urged the Court to obviate the need for such an assertion by denying the Plaintiff’s request for access on legal grounds. *See* ECF No. 264 at 4, 9–14, 18; ECF No. 269 at 2, 15; *see also* n.1, *supra*.

Because the Plaintiff’s request and the Order to Show Cause remain pending, the Government has proceeded with the consideration of whether to assert the state secrets privilege to protect the Classified Steinbach Declaration. That process has now been completed, and the

Attorney General has invoked the state secrets privilege to protect the classified information in the Classified Steinbach Declaration. *See* AG Decl. ¶ 3.

III. CATEGORIES OF INFORMATION SUBJECT TO THE ATTORNEY GENERAL'S ASSERTION OF PRIVILEGE

After careful personal consideration of the matter, *id.* ¶ 3, the Attorney General has asserted the state secrets privilege to protect the following categories of classified national security information that appear in the Classified Steinbach Declaration:

- (i) **Information Regarding National Security Legal Process that Has Been Served on Twitter.** Information regarding national security legal process that has been served on Twitter, including not only the quantity and type of any such process, but also particular information regarding the subject matter of certain FBI national security investigations as well as the communications targeted with national security legal process.
- (ii) **Information Regarding How Adversaries May Seek to Exploit Information Reflecting the Government's Use of National Security Legal Process.** Information describing how adversaries might exploit provider-specific data regarding receipt of national security legal process, both with respect to Twitter and with respect to any other provider.
- (iii) **Information Regarding the Government's Investigative and Intelligence Collection Capabilities.** Information that would reveal or tend to reveal the Government's collection capabilities.
- (iv) **Information Concerning the FBI's Investigation of Adversaries and Awareness of their Activities.** Information revealing specific targets of investigation and activities of adversaries of the United States.

Id. ¶ 4.

IV. ARGUMENT

The privilege for military and state secrets to protect information vital to the national security "is well established," and may be invoked by the Government where it is shown, "from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security, should not be divulged." *United States v. Reynolds*, 345 U.S. 1, 6-7, 10 (1953). Here, the Attorney General, after careful personal consideration of the matter, has concluded that disclosure of the four categories of information described above and in more detail in the Classified McGarrity Declaration reasonably could be expected to cause significant harm to the national security, and

1 has therefore asserted the state secrets privilege over those categories of information. *See* AG
2 Decl. ¶¶ 3–5.

3 The Court of Appeals has explained that analyzing a Government assertion of the state
4 secrets privilege involves three steps: “First [a court] must ‘ascertain that the procedural
5 requirements for invoking the state secrets privilege have been satisfied.’ Second, [a court] must
6 make an independent determination whether the information is privileged . . . Finally, ‘the
7 ultimate question to be resolved is how the matter should proceed in light of the successful
8 privilege claim.’” *Jeppesen*, 614 F.3d at 1080 (quoting *Al-Haramain Islamic Found., Inc. v.*
9 *Bush*, 507 F.3d 1190, 1202 (9th Cir. 2007)).

10 Section A below addresses the first and second steps of the analysis, and explains why
11 the Government has properly invoked the state secrets privilege in this case. Section A.1
12 discusses, to the extent possible in unclassified terms, the sensitivity of the information over
13 which the Attorney General has asserted privilege, and Section A.2 explains the national security
14 harm that reasonably could be expected to result from the disclosure of such information to
15 cleared counsel. Section A.3 then describes the extraordinary lengths to which Defendants have
16 gone to facilitate resolution of the merits of Plaintiff’s claims, and explains that the Defendants
17 have asserted the privilege “no more frequently [or] sweepingly than necessary” in this case. *Id.*
18 at 1082. As explained below, the Government has invoked the privilege now because Plaintiff’s
19 demand for access to the Classified Steinbach Declaration remains pending and the Order to
20 Show Cause has not been discharged. In light of these circumstances, the Attorney General has
21 determined that an assertion of the state secrets privilege is necessary to protect against an order
22 calling for the disclosure of “matters which, in the interest of national security, should not be
23 divulged.” *Reynolds*, 345 U.S. at 10.

24 Finally, Sections A.4 and B discuss the effects of the Government’s proper invocation of
25 privilege on these proceedings. As explained below, the privileged information is at the very
26 heart of this litigation and Plaintiff’s claims cannot “be litigated without relying on evidence that
27 would necessarily reveal those secrets or press so closely upon them as to create an unjustifiable
28 risk that they would be revealed.” *Jeppesen*, 614 F.3d at 1085. Accordingly, unless the Court

discharges the Order to show cause on other grounds presented by Defendants and thus avoids the need to reach the state secrets privilege assertion, binding precedent requires that Plaintiff's claims now be dismissed. "While dismissal of an action based on the state secrets privilege is harsh, the results are harsh in either direction and the state secrets doctrine finds the greater public good—ultimately the less harsh remedy—to be dismissal." *Kasza*, 133 F.3d at 1167 (quotation omitted).

A. The Attorney General has Properly Invoked the State Secrets Privilege to Protect the Sensitive National Security Information in the Classified Steinbach Declaration.

As discussed above, when assessing an assertion of the state secrets privilege, a court must determine whether the privilege has been properly invoked, first, procedurally, and, second, substantively. Both requirements have been fulfilled here.

With respect to the first step, "there must be a formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer." *Jeppesen*, 614 F.3d at 1080 (quoting *Reynolds*, 345 U.S. at 7–8). This requirement is indisputably met here. The Government has submitted a formal claim of privilege through the public declaration of the Attorney General, the head of the Department of Justice, following his personal consideration of the matters at issue. *See* AG Decl. ¶ 3. The Attorney General's claim of privilege is supported, in extensive detail, by the classified declaration of Acting EAD McGarrity, which explains the nature of the information at issue and the specific harms that reasonably could be expected to result from its disclosure. *See* Classified McGarrity Decl. The unclassified declaration of Acting EAD McGarrity describes those categories of information, and explains the potential harms of disclosure, to the extent possible on the public record. *See* Unclassified McGarrity Decl. ¶¶ 23–40.

Turning to the second step of the analysis, the Court must assess whether "from all the circumstances of the case . . . there is a reasonable danger that compulsion of the evidence will expose matters which, in the interest of national security, should not be divulged." *Reynolds*, 345 U.S. at 10; *Al-Haramain Islamic Found.*, 507 F.3d at 1196; *Jeppesen*, 614 F.3d at 1080. The Court must "assure itself that an appropriate balance is struck between protecting national

security matters and preserving an open court system.” *Jeppesen*, 614 F.3d at 1081 (quoting *Al-Haramain Islamic Found.*, 507 F.3d at 1203); *see also id.* at 1082 (courts should review the Government’s privilege assertions “with a very careful” and “skeptical” eye) (quotations omitted). However, “[i]n evaluating the need for secrecy,” the Ninth Circuit also has “acknowledge[d] the need to defer to the Executive on matters of foreign policy and national security” and noted that a court “surely cannot legitimately find [itself] second guessing the Executive in this arena.” *Id.* at 1081–82 (quoting *Al-Haramain Islamic Found.*, 507 F.3d at 1203); *see also e.g., Holder v. Humanitarian Law Project*, 561 U.S. 1, 34 (2010) (“when it comes to collecting evidence [on national security matters], the lack of competence on the part of the courts is marked, and respect for the Government’s conclusions is appropriate”) (quotation and citation omitted); *CIA v. Sims*, 471 U.S. 159, 180 (1985) (“[I]t is the responsibility of the [Executive], not that of the judiciary, to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the Agency’s intelligence-gathering process.”). Thus, even in situations where the privileged information may appear to be “somewhat innocuous,” the Court of Appeals has cautioned that “[the Court’s] judicial intuition . . . is no substitute for the documented risks and threats posed by the potential disclosure of national security information.” *Al-Haramain Islamic Found.*, 507 F.3d at 1203.

To allow the Court properly to complete this step of the analysis, the Government’s assertion of privilege “must be presented in sufficient detail for the court to make an independent determination of the validity of the claim of privilege and the scope of the evidence subject to the privilege.” *Jeppesen*, 614 F.3d at 1080. Here, the classified declaration of Acting EAD McGarrity describes in classified detail the information at issue, and the reasons why its disclosure reasonably could be expected to cause significant—serious, or, in some cases, exceptionally grave—damage to the national security. *See* Classified McGarrity Decl. To the extent possible, the Attorney General and Acting EAD McGarrity also describe in their public declarations the four categories of information at issue, and the harm that reasonably expected to

1 be wrought by its disclosure; however, further detail regarding each category and the potential
2 harm of its disclosure are set forth in the classified declaration of Acting EAD McGarrity.

3 **1. Disclosure of the Information at Issue Reasonably Could Be Expected to Result**
4 **in Significant Harm to the National Security.**

5 The first category of information at issue is classified detail regarding national security
6 legal process that has been served on Plaintiff, including (i) particular information regarding the
7 subject matter of certain FBI national security investigations and communications targeted with
8 national security legal process and (ii) detail regarding the quantity of national security legal
9 process that Plaintiff has received. *See* AG Decl. ¶ 6; Unclassified McGarrity Decl. ¶ 23. While
10 the first type of information in this category cannot be described in the unclassified setting, the
11 nature of the information and the reasons why its disclosure reasonably could be expected to
12 cause serious damage to the national security are discussed in the classified declaration of Acting
13 EAD McGarrity.

14 The second type of information in this category consists of detail regarding the quantity
15 of national security legal process that Plaintiff has received. Such information would reveal or
16 tend to reveal information about the extent, scope, and reach of the Government's national
17 security collection capabilities and investigative interests. AG Decl. ¶ 7; Unclassified McGarrity
18 Decl. ¶ 25. The disclosure of such information would allow adversaries of the United States,
19 including current and future targets of FBI national security investigations, significant insight
20 into the U.S. Government's counterterrorism and counterintelligence efforts and capabilities, or,
21 significantly, the lack thereof; and into particular intelligence sources and methods. AG Decl.
22 ¶ 7; Unclassified McGarrity Decl. ¶ 25.

23 More specifically, by detailing the amount of each particular type of process that Plaintiff
24 had received during a particular period, and over time, this data would reveal the extent to which
25 Twitter was or was not a safe channel of communication for our adversaries. AG Decl. ¶ 8;
26 Unclassified McGarrity Decl. ¶ 27. The Director of National Intelligence ("DNI") declassified
27 certain aggregate data formats reflecting the Government's use of national security legal process
28 to permit public reporting by recipients of such process in a manner that would increase

transparency without creating an unjustifiable risk of harm to national security. AG Decl. ¶ 8; Unclassified McGarrity Decl. ¶ 26. But the disclosure of data regarding the receipt of national security legal process by Twitter that is more granular than that which has been declassified by the DNI would reveal such information as: (i) incremental increases or decreases in collection, which would show whether the Government has a significant presence or investigative focus on a particular platform; (ii) the collection of content or non-content information, which would show whether and to what extent the Government is collecting certain types of information on that platform; and (iii) the fact of whether or when the recipient received a particular type of process at all, which may reflect different collection capabilities and focus on that platform, different types of information collected, and locations of FBI targets. AG Decl. ¶ 8; Unclassified McGarrity Decl. ¶ 26.

The second category of information as to which the Attorney General has asserted privilege includes details of how adversaries might exploit provider-specific data regarding receipt of national security legal process. AG Decl. ¶ 9; Unclassified McGarrity Decl. ¶ 28. As Acting EAD McGarrity explained, although some sophisticated adversaries may already have strategies for exploiting this kind of data, disclosure of this category of information would be tantamount to providing adversaries an instruction manual for how they can effectively take steps against the U.S. Intelligence Community. Unclassified McGarrity Decl. ¶ 28. The information within this category could be used to draw inferences from provider-specific data about the Government's collection efforts and guide adversaries to sophisticated strategies to employ in their activities against the Intelligence Community. AG Decl. ¶ 9; Unclassified McGarrity Decl. ¶ 28.

The third category of information as to which Attorney General has asserted privilege is information that would reveal or tend to reveal the Government's collection capabilities. AG Decl. ¶ 10; Unclassified McGarrity Decl. ¶ 30. Particularly where there are multiple communication options to choose from and additional services that may come on the market, if adversaries are able to discern the Government's collection capabilities and deduce which platforms are safest for their communications, they can reasonably be expected to leave

platforms where the Government has collection capability in favor of the “safe” communications channels, likely resulting in a loss of intelligence. AG Decl. ¶ 10; Unclassified McGarrity Decl. ¶ 30.

The fourth category of information as to which Attorney General has asserted privilege is information revealing specific investigative targets and activities of adversaries of the United States. AG Decl. ¶ 11; Unclassified McGarrity Decl. ¶ 31. The particularized descriptions of these targets and activities contained in the Classified Steinbach Declaration reveal not only the Government’s awareness of the activity described in each instance, but, more importantly, disclose to adversaries that those activities were subject to Government surveillance as well as the Government’s intelligence sources and methods used to acquire that information. AG Decl. ¶ 11; Unclassified McGarrity Decl. ¶ 31. The disclosure of the identities of investigative targets would alert those targets to the Government’s interest in their activities and cause them to alter their conduct to avoid detection of their future activities, which would seriously impede efforts to gain further intelligence on their activities. AG Decl. ¶ 12; Unclassified McGarrity Decl. ¶ 32. Similarly, the disclosure of information that would tend to describe, reveal, confirm or deny the existence or use of sources and methods of surveillance would again enable subjects to evade detection and, more generally, provide insights into how the Government undertakes investigations – and thereby damage future investigations that might rely on similar methods. AG Decl. ¶ 12; Unclassified McGarrity Decl. ¶ 32.

For these reasons, and the reasons discussed in the classified declaration of Acting EAD McGarrity, disclosure of the four categories of information over which the Attorney General has asserted privilege reasonably could be expected to cause significant damage to the national security. Courts considering Government claims of the state secrets privilege have recognized that the disclosure of information that reveals or tends to reveal the targets of Government surveillance or intelligence sources and methods would be harmful to national security. *See, e.g., Al-Haramain Islamic Found.*, 507 F.3d at 1203–04 (targets of Government surveillance); *Halkin v. Helms*, 598 F.2d 1, 9 (D.C. Cir. 1978) (same); *Wikimedia Found. v. NSA*, 2018 WL 3973016, at *12 (D. Md. Aug. 20, 2018) (same); *Jeppesen*, 614 F.3d at 1086 (sources and *Twitter, Inc. v. Barr, et al.*, Case No. 14-cv-4480-YGR

16
 Defs.’ Req. that the Court Discharge the Order to Show Cause and
 Deny Pl.’s Req. for Access to the Classified Steinbach Decl., or in the Alternative,
 Motion to Dismiss in Light of the Attorney General’s Assertion of the State Secrets Privilege

1 methods of CIA intelligence activities); *El-Masri v. United States*, 479 F.3d 296, 308-09 (4th
2 Cir. 2007) (same).

3 **2. Disclosure to Cleared Counsel Would Create the Risks of Harm Discussed** 4 **Herein.**

5 The Attorney General has determined that the risk of harm to national security exists
6 notwithstanding that the disclosure demanded here would be to Plaintiff's counsel who has
7 received a favorable suitability determination. *See* AG Decl. ¶ 13; Unclassified McGarrity Decl.
8 ¶ 33–40. Even in these circumstances, the Ninth Circuit has recognized that the Government
9 might still have “a legitimate interest in shielding [classified] materials even from someone with
10 the appropriate security clearance.” *Al-Haramain Islamic Found., Inc. v. U.S. Dep’t of Treasury*,
11 686 F.3d 965, 983 (9th Cir. 2012). Likewise, in upholding the dismissal of claims based on an
12 assertion of the state secrets privilege in *Jeppesen*, the Ninth Circuit emphasized that its
13 conclusion that “further litigation presents an unacceptable risk of disclosure of state secrets . . .
14 holds no matter what protective procedures the district court might employ.” *Jeppesen*, 614 F.3d
15 at 1089 (rejecting as insufficient, in the circumstances presented, “the use of devices such as
16 protective orders or restrictions on testimony”); *see also id.* at 1086 (citing the risk “that
17 compelled or inadvertent disclosure of [the privileged information at issue] in the course of
18 litigation would seriously harm legitimate national security interests”). Indeed, there is legion
19 case law rejecting access by private counsel to information over which the Government has
20 asserted the state secrets privilege.⁴

21
22
23 ⁴ *See El-Masri*, 479 F.3d at 311 (denying private counsel access to classified information
24 in state secrets case); *Sterling v. Tenet*, 416 F.3d 338, 348 (4th Cir. 2005) (same); *Ellsberg v.*
25 *Mitchell*, 709 F.2d 51, 61 (D.C. Cir. 1983) (“It is well settled that a trial judge called upon to
26 assess the legitimacy of a state secrets privilege claim should not permit the requester’s counsel
27 to participate in an *in camera* examination of putatively privileged material.”); *see also Halkin*,
28 598 F.2d at 7 (“However helpful to the court the informed advocacy of the plaintiffs’ counsel
may be, we must be especially careful not to order any dissemination of information asserted to
be privileged state secrets.”); *Tilden v. Tenet*, 140 F. Supp. 2d 623, 626 (E.D. Va. 2000)
 (“[C]ourts have routinely denied attorneys’ requests to participate in *in camera* reviews even
when the attorneys have security clearances.”).

1 Here, the Attorney General has determined that the classified information set forth in the
 2 Classified Steinbach Declaration, over which the Attorney General has asserted privilege, should
 3 be protected from disclosure even to private counsel who has passed a background investigation.

4 The recognition that a suitability determination alone is insufficient adequately to protect
 5 classified information is built into the very structure of Executive Order 13526.⁵ Executive
 6 Order 13526 provides that a person *may* have access to classified information provided that a
 7 favorable determination of eligibility for access has been made by an agency head or the agency
 8 head's designee; the person has signed an approved nondisclosure agreement; and the person has
 9 a need-to-know the information. Unclassified McGarrity Decl. ¶ 35 (citing Executive Order
 10 13526, § 4.1 (a)). Under Executive Order 13526, a "need-to-know" is "a determination within
 11 the executive branch in accordance with directives issued pursuant to this order that a
 12 prospective recipient requires access to specific classified information in order to perform or
 13 assist in a lawful and authorized governmental function." Executive Order 13526, § 6.1 (dd).
 14 This requirement is a critical facet of the protection of classified information, because it ensures
 15 that classified information is not disseminated beyond the extent to which dissemination is
 16 necessary for the Government to carry out its national security functions. Unclassified
 17 McGarrity Decl. ¶ 36. Because every additional disclosure increases the risk of unauthorized
 18 disclosure, it is important to keep to a minimum the number of people who have access to
 19 classified information. *Id.* Thus, Executive Order 13526 provides that disclosure is to be
 20 permitted if and only if there is an Executive Branch finding that a person's access is necessary
 21 to perform or assist in a governmental function. *Id.* This provision reflects the judgment that
 22 any disclosure beyond that which is necessary for the Government to carry out its functions
 23 creates an unjustifiable risk to the national security. *Id.*

24 In this case, both EAD Ghattas and Acting EAD McGarrity have determined that
 25 Plaintiff's counsel lacks the required "need-to-know" to access the sensitive national security

26 ⁵ As Defendants have explained in prior briefing, the Constitution confers on the
 27 Executive the exclusive responsibility for the protection and control of national security
 28 information. *See Egan*, 484 U.S. at 527; *Dorfmont*, 913 F.2d at 1401. Executive Order 13526
 was promulgated pursuant to that constitutional authority.

information at issue. *See* Aug. 8, 2017 Ghattas Decl. ¶¶ 17–18; Unclassified McGarrity Decl. ¶ 35. Moreover, the Attorney General has now asserted the state secrets privilege to protect that information based on his determination that the disclosure of such information to private counsel in civil actions such as this reasonably could be expected to risk or result in inadvertent, involuntary, or intentional disclosures that could cause serious or, in some cases, exceptionally grave damage to national security. AG Decl. ¶ 13. This determination supersedes any determination by a lower level Executive Branch official concerning counsel’s suitability for access. Unclassified McGarrity Decl. ¶ 42.

The determination that disclosure to counsel would create an unjustifiable risk of harm to the national security is not based on an individualized finding as to the trustworthiness of Plaintiff’s counsel, but on a recognition that any disclosure of classified national security information carries an inherent risk of harm. *Id.* ¶ 38. Plaintiff’s counsel does not seek access to classified information in order to assist the government in its functions, but to represent a private party in this civil lawsuit. *Id.* If access to classified information were extended to cleared private counsel for non-government parties in civil litigation, then private parties would have the ability to vastly extend the distribution of classified information outside of the Government on topics of their choice, simply by bringing lawsuits that put such information at issue. *Id.* This, in turn, would substantially compound the already existing risks of inadvertent, involuntary, or even intentional disclosures by holders of classified information. *Id.* Private attorneys have obligations to non-government clients that may naturally result in pushing the boundaries of what must be protected and what may be permissibly disclosed. *Id.* Private parties in civil litigation are also likely to have less familiarity with the necessary safeguards to protect classified information, including in conversations with other persons, at court hearings, or in privileged notes and work product on computers to which the Government would have no access. *Id.* Access by private counsel in civil cases would also create potential non-governmental individual marks for foreign adversaries to target in their quest to access classified information. *Id.*

1 Private counsel also stand apart from Government employees granted access to classified
2 information in performing their governmental duties, whose computers or other modes of access
3 can be closely monitored or restricted, and whose mishandling of classified information can be
4 sanctioned more directly. *Id.* ¶ 39. The Government undertakes significant measures to protect
5 classified and sensitive information from disclosure, including by training its employees how to
6 handle it, utilizing classified computer networks and Sensitive Compartmented Information
7 Facilities (SCIFs) to store it, and mandating periodic background reinvestigations of personnel
8 with access to it. *Id.* Even with such safeguards in place, it is a constant challenge to protect
9 classified information from inadvertent or intentional unauthorized disclosures. *Id.* Exposing
10 classified information to private attorneys in cases such as this is among the significant risks that
11 the “need-to-know” standard is designed to protect against. *Id.*

12 The lack of a need-to-know determination for obtaining access to classified information
13 is especially significant where Plaintiff’s counsel has never previously had access to the
14 information at issue. *Id.* ¶ 40. At most, Plaintiff Twitter has some limited information about
15 national security legal process it may have received from the Government, but it does not know
16 (or have any need to know) the background of any investigations at issue or other additional
17 background and level of detail set forth in the Classified Steinbach Declaration. *Id.* Neither
18 Plaintiff nor its counsel have the information regarding the national security threats facing the
19 United States from foreign adversaries described in the Classified Steinbach Declaration, nor
20 particular information about Government collection capabilities also described therein, nor the
21 classified analytical assessment set forth in that declaration as to how more granular disclosures
22 about legal process that may – or may not – have been served on particular communication
23 platforms could be exploited by a foreign power, resulting in significant harm to the United
24 States. *Id.* This kind of highly sensitive national security information, including about
25 counterterrorism and counterintelligence matters, is strictly controlled even within the FBI and
26 Intelligence Community and is certainly not shared with counsel in private civil lawsuits based
27 solely on a suitability determination. *Id.* In sum, even limited disclosure of the information at
28

1 issue here to Plaintiff's private counsel would be unprecedented and would risk significant harm
2 to national security. *Id.*

3 **3. The State Secrets Privilege Has Been Asserted Only to the Extent Necessary in**
4 **this Matter.**

5 The state secrets privilege is to be "asserted no more frequently and sweepingly than
6 necessary." *Jeppesen*, 614 F.3d at 1082. Sections A.1 and A.2 above, as well as Acting EAD
7 McGarrity's classified declaration, explain why it is necessary, and in the interest of national
8 security, to protect from disclosure the four categories of information at issue here. Furthermore,
9 a review of the procedural history of this case demonstrates that the Government has gone to
10 extraordinary lengths to facilitate the adjudication of the merits of Plaintiff's claims, and has not
11 invoked the state secrets privilege until it became necessary to do so to protect against a potential
12 order of disclosure.

13 Although the state secrets privilege may properly be invoked before specific disputes
14 regarding the disclosure of information have arisen, including where the Government concludes
15 that a case cannot be litigated without risking the disclosure of information that would create a
16 significant risk of harm to national security, *see, e.g. Jeppesen*, 614 F.3d at 1081, the
17 Government did not seek to invoke the state secrets privilege at the outset of this case. Rather,
18 throughout this litigation, the Government has urged the Court to proceed as in *Stillman* and its
19 progeny, which provide a way for the Court to adjudicate the merits of Plaintiff's claims without
20 the risk of harm attendant to the disclosure of such sensitive information to a private party's
21 counsel, *see supra* Section A.2. After the Court ordered the Government to submit its classified
22 explanation of the harm that reasonably could be expected to arise from Plaintiff's proposed
23 disclosure, the Government provided a classified submission, containing TOP SECRET and
24 Sensitive Compartment Information, *See* Aug. 8, 2017 Ghattas Decl. ¶ 17, solely for the Court's
25 review *ex parte*, *in camera*. *See supra* 3, 7. When the Court denied the Government's summary
26 judgment motion, the Government even suggested the entry of judgment *against* the
27 Government, based on the belief that the standard of First Amendment scrutiny being applied by
28 the Court is in error, and because further review would obviate the question of whether this case

requires either security clearances or a state secrets privilege assertion. *See* ECF No. 174 at 17 (“Under these circumstances, rather than proceed by ordering discovery, the Court should convert its July 6, 2017 Order [denying Defendants’ motion for summary judgment] to a final judgment”). The Government also has proceeded with discovery, producing nearly thirty thousand pages of materials from unclassified systems, and a log identifying classified documents collected by the FBI in its SECRET enclave in response to Plaintiff’s discovery demands, consisting of four volumes addressing email and attachments comprising over 700 pages, as well as two additional logs addressing Instant Messages and electronic documents. *See* Fourth Updated Joint Case Management Statement, ECF No. 244 at 11. Additionally, Defendants have reviewed thousands of documents from their remaining classified systems, and are continuing to prepare logs identifying responsive classified documents, to be produced to the Plaintiff on March 22. Even in the face of the requirements that classified systems be searched and reviewed, and that information about classified documents be logged, the Government had not yet asserted the state secrets privilege.

Rather, the Government has asserted the privilege now in response to the continued pendency of the Plaintiff’s request for access to the Classified Steinbach Declaration, and the Order to Show Cause why it should not be disclosed, because it appears that the Court otherwise may imminently enter an order of disclosure.⁶ In light of these circumstances, the Government has now invoked the state secrets privilege to protect the sensitive information at issue.

4. The Proper Invocation of Privilege Over These Categories of Information Renders Them Unavailable for Any Purpose in this Litigation.

Sections A.1–A.3 above set forth the reasons why the Attorney General has properly asserted the state secrets privilege to protect the classified information in the Classified Steinbach Declaration, discussed herein. If the privilege assertion is reached and upheld, those

⁶ If the Court proceeded to enter an order of disclosure notwithstanding the Government’s assertion of privilege, any such order would be subject to immediate appellate review. *See In re Copley Press, Inc.*, 518 F.3d 1022, 1025 (9th Cir. 2008); *Admiral Ins. Co. v. U.S. Dist. Court*, 881 F.2d 1486, 1491 (9th Cir. 1989); *see also, e.g., Stillman*, 319 F.3d at 547–49 (reviewing and reversing an order that classified information be disclosed to plaintiff’s counsel in that case).

categories of information must be removed from the case entirely. “When the [G]overnment successfully invokes the state secrets privilege, ‘the evidence is completely removed from the case.’” *Jeppesen*, 614 F.3d at 1082 (quoting *Kasza*, 133 F.3d at 1166); *see also Al-Haramain Islamic Found.*, 507 F.3d at 1204 (“The effect of the [G]overnment’s successful invocation of privilege is simply that the evidence is unavailable, as though a witness had died.”) (quotation omitted). The state secrets privilege is absolute, and “even the most compelling necessity cannot overcome” it, as the Supreme Court has unequivocally held, *Reynolds*, 345 U.S. at 11, and as the Ninth Circuit has recognized, *see Al-Haramain Islamic Found.*, 507 F.3d at 1204 (“The privilege, once found to exist, cannot be compromised by any showing of need on the part of the party seeking the information.”); *Kasza*, 133 F.3d at 1166.

B. Because this Case Cannot Be Litigated Without the Privileged Evidence, Binding Precedent Requires that Plaintiff’s Claims Be Dismissed.

The third and final step of the analysis regarding the Government’s assertion of privilege is to consider how the matter should proceed in light of the removal of the classified evidence. *See Jeppesen*, 614 F.3d at 1082. In some cases, “simply excluding or otherwise walling off the privileged information may suffice to protect the state secrets and ‘the case will proceed accordingly, with no consequences save those resulting from the loss of evidence.’” *Id.* at 1082–83 (quoting *Al-Haramain Islamic Found.*, 507 F.3d at 1204). In others, however, “application of the privilege may require dismissal of the action,” such as where “there is no feasible way to litigate [the defendants’] alleged liability without creating an unjustifiable risk of divulging state secrets.” *Id.* at 1087. The instant case presents such a situation; as in *Jeppesen*, “any plausible effort . . . to defend” against Plaintiff’s claims would present such a risk, notwithstanding that Plaintiff may be able to state a *prima facie* case without relying on evidence excluded by the Government’s assertion of privilege. *Id.* at 1088.

The Classified Steinbach Declaration, over which privilege has now been asserted, stands at the center of this litigation, for it is essential to explaining and understanding why Twitter has no First Amendment right to publish the information in its draft Transparency Report. As described even in unclassified terms, the centrality of the privileged information to

1 these proceedings should be evident. *See supra* 10, 14–16. The first and second categories of
 2 information are squarely at the very heart of what is at issue in this matter, as they comprise
 3 detail regarding the national security process that Plaintiff has received and the sophisticated
 4 ways that adversaries could use detail about Plaintiff’s or other providers’ receipt of national
 5 security process against the U.S. Intelligence Community. *See id.* In other words, these
 6 categories include both the specific information that Plaintiff seeks to publish and the detailed
 7 discussion of what harm reasonably could be expected to arise from the disclosure of that
 8 information. The Classified Steinbach Declaration, and the specific privileged information it
 9 contains, described herein, pertains directly to the core issue of whether Twitter has a First
 10 Amendment right to publish granular information concerning national security legal process it
 11 has received.

12 Moreover, the Court, in its July 6, 2017 Order denying the Government’s summary
 13 judgment motion, indicated that, to fulfill the standard of scrutiny the Court held to be
 14 applicable,⁷ the Government’s presentation must include consideration of specific detail such as
 15 “the volume of any requests involved,” and “an articulation of the inference the Government
 16 believes can be drawn from the information Twitter itself seeks to publish.” July 6, 2017 Order
 17 at 17. In short, the Court held that Defendants would be required to present the very kind of
 18 information excluded by the privilege—and to do so in even greater detail—as the Court held
 19 that the information presented by the Government up to that point was not sufficient to fulfill the
 20 standard that the Court had applied. *See id.*

21 Moreover, where privileged state secrets are so central to the matter, any further litigation
 22 presents an unacceptable risk of disclosure. This is because, as the Ninth Circuit has recognized,
 23 “[a]dversarial litigation, including pretrial discovery of documents and witnesses and the
 24 presentation of documents and testimony at trial, is inherently complex and unpredictable.”
 25 *Jeppesen*, 614 F.3d 1089. For example, if a Government official were to sit for a deposition or
 26 take the stand and attempt to testify as to the reasons why Plaintiff’s proposed disclosure

27 ⁷ The Government continues to respectfully disagree as to the standard that should apply
 28 to Plaintiff’s claims.

reasonably could be expected to harm national security, Plaintiff “would have every incentive to probe dangerously close to the state secrets themselves.” *Id.* at 1088 (quoting *Fitzgerald v. Penthouse Int’l Ltd.*, 776 F.2d 1236, 1243 (4th Cir. 1985). Indeed, “the plaintiff and its lawyers would have every incentive to probe as close to the core secrets as the trial judge would permit. Such probing in open court would be inevitably revealing.” *Id.* (quoting *Farnsworth Cannon, Inc. v. Grimes*, 635 F.2d 268, 281 (4th Cir. 1980) (*en banc*) (*per curiam*)). And any probing question that Plaintiff could ask about the information that Plaintiff seeks to disclose in its draft Transparency Report would necessarily risk disclosure of the privileged information subject to the Attorney General’s assertion of privilege, and any answer would place privileged facts at risk. Courts have recognized that, in such circumstances, where a witness has knowledge of the privileged materials, “state secrets could be compromised even without direct disclosure by a witness.” *Id.* at 1088 (quoting *Fitzgerald*, 776 F.2d at 1243). Citing these realities, the Ninth Circuit in *Jeppesen* held that the proper invocation of the state secrets privilege required dismissal of the plaintiffs’ claims in that case. *See id.* at 1086–90. That precedent requires the same result here; in sum, because “litigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets,” it is “impossible to proceed with the litigation.” *Jeppesen*, 614 F.3d at 1083.

V. CONCLUSION

For the foregoing reasons, the Court should deny the Plaintiff’s request for access to the Classified Steinbach Declaration and discharge the Order to Show Cause. As noted, the Court may do so on legal grounds previously set forth by the Government without reaching the Attorney General’s assertion of privilege. However, if the Court is still considering whether to grant Plaintiff’s counsel access to the Classified Steinbach Declaration, it should uphold the Attorney General’s state secrets privilege assertion over the classified information in that document described above, exclude that information from the litigation, and dismiss the Second Amended Complaint on that basis.

1 Dated: March 15, 2019

Respectfully submitted,

2 JOSEPH H. HUNT
3 Assistant Attorney General

4 DAVID L. ANDERSON
5 United States Attorney

6 ANTHONY J. COPPOLINO
7 Deputy Branch Director

8 /s/ Julia A. Heiman
9 JULIA A. HEIMAN, Bar No. 241415
10 Senior Counsel
11 CHRISTOPHER HEALY
12 Trial Attorney
13 U.S. Department of Justice
14 Civil Division, Federal Programs Branch
15 P.O. Box 883
16 Washington, D.C. 20044
17 julia.heiman@usdoj.gov
18 *Attorneys for Defendants*
19
20
21
22
23
24
25
26
27
28

Exhibit A

JOSEPH H. HUNT
Assistant Attorney General
DAVID L. ANDERSON
United States Attorney
ANTHONY J. COPPOLINO
Deputy Branch Director
JULIA A. HEIMAN
Senior Counsel
CHRISTOPHER HEALY
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch

P.O. Box 883
Washington, D.C. 20044
Telephone: (202) 616-8480
Facsimile: (202) 616-8470
Email: julia.heiman@usdoj.gov

Attorneys for Defendants the Attorney General, *et al.*

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

TWITTER, INC.,

Plaintiff,

v.

WILLIAM P. BARR, United States
Attorney General, *et al.*,
Defendants.

Case No. 14-cv-4480-YGR

**DECLARATION OF
WILLIAM P. BARR,
ATTORNEY GENERAL
OF THE UNITED STATES**

Hon. Yvonne Gonzalez Rogers

I, William P. Barr, hereby state and declare as follows:

1. I am the Attorney General of the United States and the head of the United States Department of Justice (“DOJ” or “the Department”), an Executive Department of the United States. *See* 28 U.S.C. §§501, 503, 509. The purpose of this declaration is to assert, at the request

1 of the Federal Bureau of Investigation (“FBI”), and in my capacity as the Attorney General and
2 head of DOJ, a formal claim of the state secrets privilege in order to protect the national security
3 interests of the United States. The statements made herein are based on my personal knowledge,
4 on information provided to me in my official capacity, and on my evaluation of that information.

5 2. In the course of my official duties, I have been informed that the plaintiff in this
6 action, Twitter Inc. (“Twitter”), has brought First Amendment claims challenging the
7 Government’s determination that Twitter’s draft Transparency Report cannot be published
8 because it contains information regarding Twitter’s receipt of national security legal process that
9 is properly classified. I understand that following the submission of Twitter’s Second Amended
10 Complaint, the Government filed a motion for summary judgment in this matter supported by the
11 Classified Declaration of the Executive Assistant Director (“EAD”) of the FBI, Michael
12 Steinbach (the “Classified Steinbach Declaration”), after the Court had indicated that the
13 Government should include with its summary judgment motion an *ex parte* presentation in
14 support of its motion, or risk being precluded from making such a submission later. I
15 understand, further, that the Classified Steinbach Declaration was submitted for the solely for the
16 Court’s *ex parte, in camera* review.

17 3. I have read and carefully considered the public and classified declarations of
18 Michael C. McGarrity (“McGarrity Declaration”), Acting Executive Assistant Director of the
19 National Security Branch of the FBI and have reviewed the Classified Steinbach Declaration and
20 certain other filings and court orders relevant to this matter. After careful and actual personal
21 consideration of the matter, I have concluded that disclosure of the four categories of information
22 described below and in more detail in the classified McGarrity Declaration could reasonably be
23 expected to cause significant harm to the national security, and I therefore formally assert the
24 state secrets privilege over this information. The classified McGarrity Declaration, which is
25 available for the Court’s *ex parte, in camera* review, describes in classified detail the information
26 over which I am asserting the state secrets privilege. As Attorney General, I possess original
27 classification authority under Section 1.3 of Executive Order 13526, dated December 29, 2009.
28 *See* 75 Fed. Reg. 707. The classified McGarrity Declaration is properly classified under Section

1.2 of Executive Order 13526 because disclosure of the information contained in that declaration also could reasonably be expected to cause significant harm to national security.

4. In unclassified terms, my privilege assertion encompasses the following categories of sensitive national security information that appear in the Classified Steinbach Declaration:

- (i) **Information Regarding National Security Legal Process that Has Been Served on Twitter:** Information regarding national security legal process that has been served on Twitter, including not only the quantity and type of any such process, but also particular information regarding the subject matter of certain FBI national security investigations as well as the communications targeted with national security legal process.
- (ii) **Information Regarding How Adversaries May Seek to Exploit Information Reflecting the Government's Use of National Security Legal Process.** Information describing how adversaries might exploit provider-specific data regarding receipt of national security legal process, both with respect to Twitter and with respect to any other provider.
- (iii) **Information Regarding the Government's Investigative and Intelligence Collection Capabilities.** Information that would reveal or tend to reveal the Government's collection capabilities.
- (iv) **Information Concerning the FBI's Investigation of Adversaries and Awareness of their Activities.** Information revealing specific targets of investigation and activities of adversaries of the United States.

5. As indicated above and explained further below, I have determined that disclosure of information falling into the foregoing categories could reasonably be expected to cause significant harm to national security.

6. First, I agree with the FBI's assessment that disclosure of classified information regarding national security legal process that has been served on Twitter reasonably could be expected to cause significant harm to national security. My privilege assertion encompasses both types of information in this category—(i) particular information regarding the subject matter of certain FBI national security investigations and communications targeted with national security legal process, and (ii) detail regarding the quantity of national security legal process that Twitter has received. For reasons stated in the FBI's classified declaration, the disclosure of such information reasonably could be expected to cause serious damage to national security.

1 7. In particular, I agree with the FBI that the disclosure of details regarding the
2 quantity of national security legal process that Twitter has received reasonably could be expected
3 to cause significant harm to national security. As the FBI explained, such information would
4 reveal or tend to reveal information about the extent, scope, and reach of the Government's
5 national security collection capabilities and investigative interests. The disclosure of such
6 information, as the FBI explained, would allow adversaries of the United States, including
7 current and future targets of FBI national security investigations, significant insight into the U.S.
8 Government's counterterrorism and counterintelligence efforts and capabilities, or, significantly,
9 the lack thereof; and into particular intelligence sources and methods.

10 8. As the FBI explained, by detailing the amount of each particular type of process
11 Twitter had received during a particular period, and over time, this data would reveal the extent
12 to which Twitter was or was not a safe channel of communication for our adversaries. The
13 Director of National Intelligence ("DNI") declassified certain aggregate data formats reflecting
14 the Government's use of national security legal process in order to permit public reporting by
15 recipients of such process in a manner that would increase transparency while minimizing harm
16 to national security. However, as the FBI explained, the disclosure of data regarding the receipt
17 of national security legal process by Twitter that is more granular than that which has been
18 declassified by the DNI would reveal such information as: (i) incremental increases or decreases
19 in collection, which would show whether the Government has a significant presence or
20 investigative focus on a particular platform; (ii) the collection of content or non-content
21 information, which would show whether and to what extent the Government is collecting certain
22 types of information on that platform; and (iii) the fact of whether or when the recipient received
23 a particular type of process at all, which may reflect different collection capabilities and focus on
24 that platform, different types of information collected, and locations of FBI targets. Additional
25 details concerning why disclosure of information in this category reasonably could be expected
26 to cause serious damage to national security are set forth in the FBI's classified declaration.

27 9. Second, I concur with the FBI's determination that the disclosure of details of
28 how adversaries might exploit provider-specific data regarding receipt of national security legal

1 process, both with respect to Twitter and with respect to any other provider, reasonably could be
2 expected to cause significant harm to national security. I agree with the FBI's judgment that,
3 because the information within this category could be used to draw inferences from provider-
4 specific data about the Government's collection efforts and guide adversaries to sophisticated
5 strategies to employ in their activities against the Intelligence Community, its disclosure
6 reasonably could be expected to cause serious damage to the national security.

7 10. Third, I agree with the FBI that disclosure of information that would reveal or
8 tend to reveal the Government's collection capabilities reasonably could be expected to cause
9 significant harm to national security. As the FBI explained, particularly where there are multiple
10 communication options to choose from and additional services that may come on the market, if
11 adversaries are able to discern the Government's collection capabilities and deduce which
12 platforms are safest for their communications, they can reasonably be expected to leave
13 platforms where the Government has collection capability in favor of the "safe" communications
14 channels, likely resulting in a loss of intelligence. The specific information that falls into this
15 category, and further reasons why its disclosure reasonably could be expected to cause serious
16 damage to national security, are set forth in the FBI's classified declaration.

17 11. Fourth, I agree with the FBI's determination that disclosure of information
18 revealing specific targets of investigation and activities of adversaries of the United States
19 reasonably could be expected to cause significant harm to national security. As the FBI
20 explained, the particularized descriptions of these targets and activities contained in the
21 Classified Steinbach Declaration reveal not only the Government's awareness of the activity
22 described in each instance, but, more importantly, would disclose to adversaries that those
23 activities were subject to Government surveillance as well as the Government's intelligence
24 sources and methods used to acquire that information.

25 12. In particular, as the FBI noted, the disclosure of the identities of investigative
26 targets would alert those targets to the Government's interest in their activities and cause them to
27 alter their conduct to avoid detection of their future activities, which would seriously impede
28 efforts to gain further intelligence on their activities. Similarly, as the FBI further explained, the

1 disclosure of information that would tend to describe, reveal, confirm or deny the existence or
2 use of sources and methods of surveillance would again enable a subject to evade detection and,
3 more generally, provide insights into how the Government undertakes investigations – and
4 thereby damage future investigations that might rely on similar methods. I agree with the FBI's
5 assessment that either outcome reasonably could be expected to cause serious or exceptionally
6 grave damage to national security by denying the United States access to information crucial to
7 the defense of the United States both at home and abroad.

8 13. Finally, I have determined that the foregoing categories of information should be
9 protected from disclosure in this litigation pursuant to this privilege assertion regardless of the
10 fact that counsel for Twitter has completed one aspect of the security clearance process, a
11 favorable background investigation. As the FBI explains, the detailed, comprehensive, and
12 highly classified information in EAD Steinbach's classified declaration was intended solely for
13 the Court's *ex parte, in camera* review, and the disclosure of such information to private counsel
14 in civil actions such as this reasonably could be expected to risk or result in inadvertent,
15 involuntary, or intentional disclosures that could cause serious, or in some cases, exceptionally
16 grave damage to national security. I therefore assert the state secrets privilege over that
17 classified declaration in my capacity as the head of the Department of Justice and thereby
18 formally object to its disclosure to Plaintiff's counsel.

19 14. Any further elaboration on the public record concerning the four categories of
20 classified national security information at issue here, and the harm that reasonably could be
21 expected from their disclosure, would reveal information that could cause the very harms my
22 assertion of the state secrets privilege is intended to prevent. The classified McGarrity
23 Declaration, submitted for *ex parte, in camera* review, provides a more detailed explanation of
24 the information over which I am asserting the privilege and the harms to national security that
25 reasonably could be expected to result from disclosure of that information.

26 15. Under the *Attorney General's Policies and Procedures Governing Invocation of*
27 *the State Secrets Privilege* (Sept. 23, 2009) ("State Secrets Guidance"), the Department of Justice
28 will defend an assertion of the state secrets privilege in litigation, and seek dismissal of a claim

on that basis, only when “necessary to protect against the risk of significant harm to national security.” *See* Exhibit 1 (State Secrets Guidance), ¶ 1(A). The policy provides further that an application of a privilege assertion must be narrowly tailored and that dismissal be sought pursuant to the privilege assertion only when necessary to prevent significant harm to national security. *Id.* ¶ 1(B). Moreover, “[t]he Department will not defend an invocation of the privilege in order to: (i) conceal violations of the law, inefficiency, or administrative error; (ii) prevent embarrassment to a person, organization, or agency of the United States government; (iii) restrain competition; or (iv) prevent or delay the release of information the release of which would not reasonably be expected to cause significant harm to national security.” *Id.* ¶ 1(C). The policy also establishes detailed procedures for review of a proposed assertion of the state secrets privilege in a particular case. *Id.* ¶ 2. Those procedures require submissions by the relevant government departments or agencies specifying “(i) the nature of the information that must be protected from unauthorized disclosure; (ii) the significant harm to national security that disclosure can reasonably be expected to cause; [and] (iii) the reason why unauthorized disclosure is reasonably likely to cause such harm.” *Id.* ¶ 2(A). Based on my personal consideration of the matter, I have determined that the requirements for an assertion and defense of the state secrets privilege have been met in this case in accord with the Department’s State Secrets Guidance.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on this 15th day of March, 2019.



 WILLIAM P. BARR
 Attorney General of the United States

Exhibit B

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

| | | |
|-------------------------------|---|----------------------------|
| TWITTER, INC., |) | |
| Plaintiff, |) | |
| |) | Docket No. 14-cv-04480-YGR |
| v. |) | |
| |) | |
| WILLIAM BARR, <i>et al.</i> , |) | |
| |) | |
| Defendants. |) | |

UNCLASSIFIED DECLARATION OF MICHAEL C. MCGARRITY

I, Michael C. McGarrity, hereby declare as follows, pursuant to 28 U.S.C. § 1746:

I. INTRODUCTION

1. I am the Acting Executive Assistant Director (“EAD”) of the National Security Branch of the Federal Bureau of Investigation (“FBI”), United States Department of Justice. The purpose of this declaration is to support an assertion of the military and state secrets privilege (“state secrets privilege” or “the privilege”) by the Attorney General in the above captioned case.¹
2. As the Acting Executive Assistant Director of the FBI’s National Security Branch, I am responsible for, among other things, overseeing the national security operations of the FBI’s Counterintelligence Division, Counterterrorism Division, High-Value Detainee Interrogation

¹ In a separate, classified declaration, I have set forth a more thorough explanation of the reasons that support an assertion of the state secrets privilege in this matter. It is my understanding that counsel for Defendants will make the classified declaration available to the Court solely for its *ex parte* and *in camera* review by lodging that declaration with the Court Information Security Officer. The FBI does not consent to its disclosure beyond the presiding judge.

Group, Terrorist Screening Center, and Weapons of Mass Destruction Directorate. The FBI's National Security Branch also guides the functions carried out by other FBI divisions that support the FBI's national security missions, such as training, technology, human resources, and any other operations that further the FBI's mission to defeat national security threats directed against the United States. In this role, I have official supervision over all of the FBI's investigations to deter, detect, and disrupt national security threats to the United States.

3. As the Acting Executive Assistant Director of the National Security Branch, I have also been delegated original classification authority by the Director of the FBI. *See* Executive Order 13526, 75 F.R. 707 (Dec. 29, 2009), Section 1.3 (c). As a result, I am responsible for the protection of classified national security information within the National Security Branch of the FBI and in matters affecting the national security mission of the FBI, including the sources and methods used by the FBI in the collection of national security and criminal information for national security investigations. To that end, the Director of the FBI has authorized me to execute declarations and affidavits to protect such information.

4. I submit this declaration in support of an assertion of the state secrets privilege by the Attorney General in order to protect classified national security information provided to the Court in the Classified Declaration of EAD Michael B. Steinbach ("Classified Steinbach Declaration"). The purpose of the Classified Steinbach Declaration was to describe—in classified detail—the national security harms that reasonably could be expected to result from the disclosure of information that Plaintiff Twitter, Inc., ("Twitter") sought to publish in a draft Transparency Report, which I understand to be the subject of this litigation. I have personally

reviewed the Classified Steinbach Declaration. As discussed herein, the classified material contained in that declaration includes information concerning critical intelligence-gathering activities and capabilities, the disclosure of which reasonably could be expected to cause serious, or, in some cases, exceptionally grave damage to the national security of the United States.

5. The statements in this declaration are based on my personal knowledge, my review and consideration of documents and information made available to me in my official capacity, and on information obtained from Special Agents and other FBI employees. I have reached my stated conclusions in accordance with this information.

II. BACKGROUND

A. National Security Legal Process

6. Several federal statutes authorize the FBI to obtain information from individuals or private entities, including electronic communication service providers (“providers”), in furtherance of investigations conducted to protect the national security of the United States. Under 18 U.S.C. § 2709, 12 U.S.C. § 3414, and 15 U.S.C. §§ 1681u, 1681v, the FBI may issue National Security Letters (“NSLs”). The Foreign Intelligence Surveillance Act (“FISA”) provides different mechanisms for the Government to obtain foreign intelligence information in support of its national security investigations, including: Title I, authorizing electronic surveillance within the United States; Title III, allowing physical searches in the United States; Title IV, permitting the installation of pen registers and trap and trace devices; Title V, for access to certain “tangible things;” and Title VII, permitting the acquisition of foreign intelligence information concerning subjects outside the United States. *See* 50 U.S.C. §§ 1801 *et seq.*

7. This declaration refers at times collectively to NSLs and FISA orders and directives as “national security process” or “national security legal process.” In some circumstances, data reflecting the Government’s use of such process, including qualitative and quantitative information about the national security process received by a particular individual or entity, is classified and subject to nondisclosure requirements imposed by statute or court order or both.

8. I understand that Twitter filed this lawsuit in order to challenge the limitations on its ability to publicly report data reflecting specific numbers and types of national security legal process that Twitter received during the six month period from July 1 through December 31, 2013, and to publish similar data for future timeframes.

B. Provider Reporting Regarding Receipt of National Security Process

9. As EAD Steinbach explained, following unauthorized disclosures by Edward Snowden of documents that purportedly contained classified national security information, multiple providers sought to disclose data regarding their receipt of national security process to correct perceived inaccuracies in the press and to address public speculation about the nature and scope of their cooperation with the Government.

10. Citing exceptional circumstances, including the need to facilitate transparency and the impact of secrecy on providers, in 2014 and 2015, the Director of National Intelligence (“DNI”) declassified certain categories of data reflecting the Government’s use of national security process, to permit disclosure of such data by recipients of national security process if reported in one of a number of specified formats. As noted in EAD Steinbach’s Declaration, the categories of data reflecting the Government’s use of national security process declassified by the DNI in

2015 that providers and others may choose to publicly report are set forth in Section 603 of the USA FREEDOM Act and codified at 18 U.S.C. § 1874.

11. The reporting framework reflected in the 2015 DNI declassification and the USA FREEDOM Act allows providers to report aggregate data regarding their receipt of national security process with more granularity than had ever been permitted before. Under each of the permissible reporting formats recognized by Congress: (1) if a recipient of national security process chooses to publicly report quantitative information revealing that it received *any* national security process, it must report statistics regarding process received in every category of authorities, even if that provider received no process pursuant to a particular category; (2) the allowable methods of reporting are all structured as defined aggregate quantities of national security process, varying in scale depending on defined categories of national security process (“bands”); and (3) each category of reporting bands begins at “0.”

12. As EAD Steinbach explained, the currently-operative reporting framework allows electronic communication service providers and others who are subject to national security process, and the secrecy requirements that accompany such process, latitude to describe the process that they have received without unduly compromising national security interests. Information at a more granular level than described in the USA FREEDOM Act remains classified, because it would provide a roadmap to adversaries revealing the existence of or extent to which Government surveillance may be occurring at Twitter or providers like Twitter.

C. Background Regarding the Classified Steinbach Declaration

13. As stated above, I understand that Twitter filed this lawsuit in order to challenge the

limitations on its ability to publicly report data regarding its receipt of national security process under the above-referenced framework; that Twitter sought to disclose data regarding its receipt of national security process that was far more granular than that which had been declassified by the DNI; and that the Government submitted, *ex parte* and *in camera*, the Classified Steinbach Declaration in order to demonstrate for the Court that the information Twitter seeks to publish is properly classified and the harms to national security that could reasonably be expected to result from disclosure of that information. The classified content of the Classified Steinbach Declaration – the information over which the Attorney General is asserting the state secrets privilege – explains in classified terms why the data Twitter seeks to publish is more granular than permitted by the framework reflected in the USA FREEDOM Act and the DNI declassification, and why disclosure of that data reasonably could be expected to cause significant harm to national security.

14. I also have been informed that counsel for Twitter has made a request to the Court for access to the Classified Steinbach Declaration, and that the Court thereafter issued an Order to Show Cause why the Government should not be compelled to disclose the Classified Steinbach Declaration to Twitter's counsel. I also understand that to facilitate access to this classified document (and potentially other classified information in discovery), the Court previously ordered the Government to initiate a background investigation of Twitter's counsel for purposes of providing counsel with a security clearance.

15. Pursuant to the requirements of Executive Order No. 13526, former EAD Carl Ghattas, a predecessor in this role, reviewed the Classified Steinbach Declaration and, as discussed in

greater detail in Section V, below, determined that, although the background investigation of Twitter's counsel was favorably adjudicated, he does not meet the requirements for access to the classified FBI information at issue in this case on the grounds that counsel does not have a "need-to-know" that information.

16. The Attorney General is asserting the state secrets privilege to protect the Classified Steinbach Declaration from disclosure. The remainder of this declaration supports the Attorney General's assertion of the state secrets privilege in this case by explaining the harms to national security that reasonably could be expected to result from the unauthorized disclosure of the Classified Steinbach Declaration.

III. SUMMARY

17. I have determined that the information described below, contained in paragraphs portion-marked as classified in the Classified Steinbach declaration, is properly classified and that its unauthorized disclosure reasonably could be expected to result in exceptionally grave (Top Secret-marked) or serious (Secret-marked) damage to the national security.
18. In unclassified terms, the classified information contained in the Classified Steinbach declaration, and subject to the Attorney General's state secrets privilege assertion, includes the following four categories of classified information:
- (1) Information regarding national security process that has been served on Twitter;
 - (2) Information regarding how adversaries may seek to exploit information reflecting the Government's use of national security process, including disclosures by recipients of any such process;
 - (3) Information regarding the Government's investigative and intelligence collection capabilities; and

(4) Information concerning the FBI's investigation of adversaries and awareness of their activities, including sources and methods of investigation and intelligence collection concerning those adversaries.

19. Disclosure of the first category of information at issue – information concerning national security legal process served on Twitter – reasonably could be expected to cause serious damage to national security. Disclosure of specific information concerning the amount and type of national security legal process received by a particular service provider would provide highly valuable insights into where and how the United States is or is not deploying its investigative resources, and would tend to reveal which communications services may or may not be secure, which types of information may or may not have been collected, and thus whether or to what extent the United States is or is not aware of the activities of these adversaries.
20. Disclosure of the next two categories of sensitive information set forth in the Classified Steinbach Declaration – detail regarding how an adversary could exploit provider disclosures regarding receipt of national security process and discussion of the Government's collection capabilities – both reasonably could be expected to cause serious damage to the national security, because they would provide a roadmap for adversaries as to how to exploit to their advantage information concerning Government intelligence collection activities.
21. Disclosure of the fourth category of sensitive information set forth in the Classified Steinbach Declaration, information concerning the FBI's investigation of adversaries and awareness of their activities, including sources and methods of investigation and intelligence collection concerning those adversaries, reasonably could be expected to cause serious, and in

some cases, exceptionally grave, damage to the national security.

22. For these reasons and others explained below and in my classified declaration, information falling within the categories described above is currently and properly classified and subject to the Attorney General's assertion of the state secrets privilege because disclosure reasonably could be expected to cause serious or exceptionally grave damage to the national security of the United States.

IV. HARM OF DISCLOSURE OF PRIVILEGED INFORMATION CONTAINED IN THE CLASSIFIED STEINBACH DECLARATION

A. Information regarding any national security legal process served on Twitter

23. The first category of classified information over which the Attorney General is asserting privilege concerns specific detail regarding any national security legal process that has been served on Twitter. This category of information includes (1) particular information regarding the subject matter of certain FBI national security investigations as well as the communications targeted with national security legal process; and (2) the quantity of any national security legal process that has been served on Twitter—such as the data contained in the draft Transparency Report at issue in this case.
24. The first type of information in this category cannot be described in greater detail in this unclassified setting. But the disclosure of the FBI investigative information at issue in this category reasonably could be expected to cause serious damage to national security.
25. The second type of information in this category at issue includes detail set forth in the Classified Steinbach Declaration regarding the quantity of national security process that Twitter has received (including information contained in Twitter's draft Transparency Report), the

disclosure of which reasonably could be expected to cause significant harm to national security. Data contained in the Classified Steinbach Declaration regarding national security legal process received by Twitter would reveal or tend to reveal information about the extent, scope, and reach of the Government's national security collection capabilities and investigative interests. The disclosure of such information would allow adversaries of the United States, including current and future targets of FBI national security investigations, significant insight into the U.S. Government's counterterrorism and counterintelligence efforts and capabilities, or, significantly, the lack thereof; and into particular intelligence sources and methods.

26. The Director of National Intelligence declassified certain aggregate quantities of data reflecting the Government's use of national security legal process to permit public reporting by recipients of such process, if reported in one of the formats specified by the Government.² Those formats were designed specifically to minimize the harms that could reasonably be expected to result from disclosure of this data if publicly reported as specific quantities and types of process or in smaller aggregate quantities. Granular data regarding the national security legal process received by Twitter, which data is contained in the Classified Steinbach Declaration, would reveal such information as: (i) incremental increases or decreases in collection, which would show whether the Government has a significant presence or investigative focus on a particular platform; (ii) the collection of content or non-content information, which would show whether

² Although DNI James R. Clapper concluded that the declassified aggregate quantities of data were properly classified because disclosure reasonably could be expected to harm national security, he elected to declassify the information in the interests of transparency and the impact of secrecy on providers.

and to what extent the Government is collecting certain types of information on that platform; and (iii) the fact of whether or when the recipient received a particular type of process at all, which may reflect different collection capabilities and focus on that platform, different types of information collected, and locations of FBI targets.

27. More specifically, by detailing the amount of each particular type of process Twitter had received during a particular period, and over time, this data would reveal the extent to which Twitter was or was not a safe channel of communication for our adversaries. It is reasonable to expect that our adversaries will take action based on such information. Even historical data would be alerting to adversaries by tending to reveal collection capabilities and investigative interests.

B. Information regarding how an adversary can exploit provider disclosures regarding receipt of national security legal process

28. The second category of classified information over which the privilege is asserted is information set forth in the Classified Steinbach Declaration that details how adversaries might exploit provider-specific data regarding receipt of national security legal process, both with respect to Twitter and with respect to any other provider. Although some sophisticated adversaries may already have strategies for exploiting this kind of data, disclosure of this category of information would be tantamount to providing adversaries an instruction manual for how they can effectively take steps against the U.S. Intelligence Community.

29. In sum, the information within this category could be used to draw inferences from provider-specific data about the Government's collection efforts and guide adversaries to sophisticated strategies to employ in their activities against the Intelligence Community, and

therefore its disclosure reasonably could be expected to cause serious damage to the national security.

C. The Government's collection capabilities

30. The third category of classified information over which the privilege is asserted is information that would reveal or tend to reveal the Government's collection capabilities. Particularly where there are multiple communication options to choose from and additional services that may come on the market, if adversaries are able to discern the Government's collection capabilities and deduce which platforms are safest for their communications, they can reasonably be expected to leave platforms where the Government has collection capability in favor of the "safe" communications channels, likely resulting in a loss of intelligence. The specific information that falls into this category, and further reasons why its disclosure reasonably could be expected to cause serious damage to national security, are set forth in my classified declaration.

D. Information regarding investigations of adversaries' activities

31. The final category of classified information over which the privilege is asserted by the Attorney General is information revealing specific investigative targets and activities of adversaries of the United States. The particularized descriptions of these targets and activities contained in the Classified Steinbach Declaration reveal not only the Government's awareness of the activity described in each instance, but, more importantly, disclose to adversaries that those activities were subject to Government surveillance. In so doing, such disclosures tend to reveal—and therefore diminish the utility of—the Government's intelligence sources and

methods used to acquire that information. The disclosure of such information reasonably could be expected to cause serious, and, in some cases, exceptionally grave damage to the national security.

32. In particular, the disclosure of the identities of investigative targets would alert those targets to the Government's interest in their activities and cause them to alter their conduct to avoid detection of their future activities, which would seriously impede efforts to gain further intelligence on their activities. Similarly, the disclosure of information that would tend to describe, reveal, confirm or deny the existence or use of sources and methods of surveillance would again enable a subject to evade detection and, more generally, provide insights into how the Government undertakes investigations – and thereby damage future investigations that might rely on similar methods. Either outcome reasonably could be expected to cause serious or exceptionally grave damage to national security by denying the United States access to information crucial to the defense of the United States both at home and abroad.

V. RISK OF HARM FROM DISCLOSURE TO CLEARED COUNSEL

33. As noted above, I have been informed that Twitter has requested that the Classified Steinbach Declaration be disclosed to its counsel. I understand that the Court previously ordered that the Government conduct a background investigation of Plaintiff's counsel in order to make a security clearance "suitability" determination, and that, after a favorable suitability determination was made, the Court entered an Order to Show Cause why the Government should not be compelled to make such a disclosure. The discussion above explains why disclosure of the foregoing categories of classified information, which are contained in the Classified Steinbach

Declaration, reasonably could be expected to cause significant—serious and in some cases exceptional—harm to national security. The remainder of this declaration addresses why counsel for Plaintiff Twitter will not be permitted access to this classified information, over which the Attorney General is asserting the state secrets privilege, even where counsel has undergone a background investigation showing that he is suitable to receive classified information.

34. In sum, and as set forth further below, a determination of trustworthiness alone is insufficient to obtain access to classified information. The Executive Branch agency responsible for the classified information must also consent to the disclosure of the information at issue, through what is called a “need-to-know” determination. The FBI objects to the disclosure of classified information to Plaintiff’s counsel in this case and has determined that counsel lacks the requisite need-to-know. Access to classified information by private counsel in civil lawsuits such as this would significantly expand access to highly sensitive information and the attendant risk of inadvertent, involuntary, or intentional disclosures that could cause serious damage to national security. The lack of a need-to-know determination for obtaining access to classified information is especially significant where Twitter’s counsel has never previously had access to any of the information set forth in the classified declaration. Finally, an assertion of the state secrets privilege by the Attorney General constitutes a judgment at the highest level of the Department of Justice that the classified FBI information at issue should be protected and excluded from the case as a matter of law, and supersedes any administrative determination by lower level officials regarding access to classified information.

35. First, in addition to a favorable suitability determination, the Executive Branch must consent to granting access to particular classified information. Here, Twitter's counsel lacks the required "need-to-know" determination to obtain access to classified information. The Executive Branch has long recognized that a reliable way to mitigate the risk of unauthorized disclosures of sensitive national security information is to limit the number of individuals who have access to it. This principle is incorporated in Executive Order 13526, which states that a person *may* have access to classified information provided that a favorable determination of eligibility for access has been made by an agency head or the agency head's designee; the person has signed an approved nondisclosure agreement; and the person has a need-to-know the information. Executive Order 13526, Sec. 4.1 (a). A need-to-know is expressly defined by the Executive Order as "a determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function." Executive Order 13526, § 6.1 (dd). The need-to-know requirement governs access by any person to classified information, including government personnel with the highest levels of clearance.

36. The need-to-know requirement is a critical facet of the protection of classified information because it ensures that classified information is not disseminated beyond the extent to which dissemination is necessary for the Government to carry out its national security functions. Because, as discussed further herein, every additional disclosure increases the risk of unauthorized disclosure, it is important to keep to a minimum the number of people who have

access to classified information. Thus, Executive Order 13526 provides that disclosure is to be permitted if and only if there is an Executive Branch finding that a person's access is necessary to perform or assist in a governmental function. This provision reflects the judgment that any disclosure beyond that which is necessary for the Government to carry out its functions creates an unjustifiable risk to the national security.

37. As discussed above, former EAD Carl Ghattas determined that Twitter's counsel does not have a "need-to-know" the classified FBI information at issue in this case, which includes the classified material contained in the Steinbach declaration, "and all classified information underlying the bases for the government's classification determinations with respect to data concerning the FBI's use of national security process." *See* Aug. 8, 2017 EAD Ghattas Decl. ¶¶ 17–18. EAD Ghattas reached this conclusion pursuant to the directives of Executive Order 13526, on the ground that "it does not serve a governmental function, within the meaning of the Executive Order, to allow plaintiff's counsel access to the classified FBI information at issue in this case to assist in representing the interest of a private plaintiff who has filed this civil suit against the government." Aug. 8, 2017 EAD Ghattas Decl. ¶ 18. Consequently, Twitter's counsel does not meet the requirements for access to the classified information, irrespective of whether the background investigation was favorably adjudicated. *Id.* I agree with EAD Ghattas' determination.

38. This determination is not based on an individualized finding as to the trustworthiness of counsel for Twitter, but on a recognition that any disclosure of classified national security information carries an inherent risk of harm, even if disclosed to persons who have received the

requisite suitability determination. For this reason, even career government employees who have received a suitability determination for access to classified information may not, by virtue of that determination, obtain access to any and all classified information absent a need-to-know particular information in the performance of a governmental function. Counsel for Twitter does not seek access to classified information in order to assist the government in its functions, but to represent a private party in this civil lawsuit. If access to classified information is extended to cleared private counsel for non-government parties in civil litigation, then private parties would have the ability to vastly extend the distribution of classified information outside of the Government on topics of their choice, simply by bringing lawsuits that put such information at issue. The already existing risks of inadvertent, involuntary, or even intentional disclosures by holders of classified information would be substantially compounded in these circumstances. Private attorneys have obligations to non-government clients that may naturally result in pushing the boundaries of what must be protected and what may be permissibly disclosed. Private parties in civil litigation are also likely to have less familiarity with the necessary safeguards to protect classified information, including in conversations with other persons, at court hearings, or in privileged notes and work product on computers to which the Government would have no access. Access by private counsel in civil cases would also create potential non-governmental individuals for foreign adversaries to target in their quest to access classified information.

39. In particular, private counsel stand apart from Government employees granted access to classified information in performing their governmental duties, whose computers or other modes of access can be closely monitored or restricted, and whose mishandling of classified information

can be sanctioned more directly. The Government undertakes significant measures to protect classified and sensitive information from disclosure, including by training its employees how to handle it, utilizing classified computer networks and Sensitive Compartmented Information Facilities (SCIFs) to store it, and mandating periodic background reinvestigations of personnel with access to it. Even with such safeguards in place, it is a constant challenge to protect classified information from inadvertent or intentional unauthorized disclosures. Exposing classified information to private attorneys in cases such as this is among the significant risks that the “need-to-know” standard is designed to protect against.

40. The lack of a need-to-know determination for obtaining access to classified information is especially significant where Twitter’s counsel has never previously had access to any of the information set forth in the Classified Steinbach Declaration. At most, Twitter has some limited information about national security legal process it may have received from the Government, but it does not know (or have any need to know) the background of any investigations at issue or other additional background and level of detail set forth in the Classified Steinbach Declaration. Neither Twitter nor its counsel have the information regarding the national security threats facing the United States from foreign adversaries described in the Classified Steinbach Declaration, nor particular information about Government collection capabilities also described therein, nor the classified analytical assessment set forth in that declaration as to how more granular disclosures about legal process that may – or may not – have been served on particular communication platforms could be exploited by a foreign power, resulting in significant harm to the United States. This kind of highly sensitive national security information, including about

counterterrorism and counterintelligence matters, is strictly controlled even within the FBI and Intelligence Community and is certainly not shared with counsel in private civil lawsuits based solely on a suitability determination. In sum, even limited disclosure of the information at issue to a private plaintiff's counsel would be unprecedented and would risk significant harm to national security.

41. It is also of particular concern to the FBI that information intended solely for an Article III judge would be turned over to private counsel. Control over the disclosure of classified information belongs to the Executive Branch and not to the Judicial Branch. The Executive Branch frequently entrusts Article III judges, confirmed by the Senate, with classified information in order for courts to perform their judicial functions. *See* 28 C.F.R. § 17.46(c). Article III judges frequently obtain classified information for *ex parte*, *in camera* review at a level of detail entrusted only to persons with a high level of security clearance, such as in the information in the Classified Steinbach Declaration and this classified declaration submitted to support the Attorney General's state secrets privilege assertion. As former EAD Ghattas explained, for district judges to order the disclosure of such highly classified information to private counsel – particularly *after* it has already been submitted solely for *ex parte*, *in camera* review – would create a severe disincentive for the Government to share highly classified information with courts to begin with, or at the least would cause agencies to reconsider the level of information they would be willing to provide a court *ex parte*. *See* Aug. 8, 2017 EAD Ghattas Decl. ¶ 20.
42. Finally, the Attorney General, as the head of the Department of Justice, is asserting the

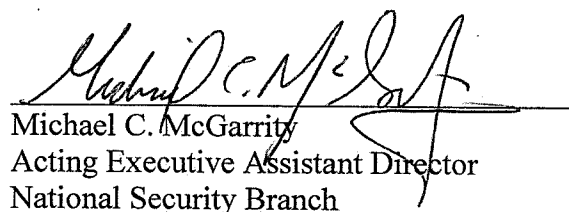
state secrets privilege in this case to protect the classified information described above, based on the determination that the particular privileged information at issue should be protected from disclosure and excluded from further proceedings in litigation in order to prevent a significant risk of harm to national security. The Attorney General's action supersedes any determination by a lower level Executive Branch official concerning access to this information in litigation.

VI. CONCLUSION

43. The information set forth in the classified portions of my classified declaration and in the classified portions of the Classified Steinbach Declaration is properly classified and extremely sensitive. The unauthorized disclosure of this information reasonably could be expected to cause either serious or exceptionally grave damage to the national security of the United States. For the reasons explained above and in my classified declaration, the assertion by the Attorney General of the state secrets privilege over this information should be sustained.

I declare under penalty of perjury that the foregoing is true and correct.

Dated: March 15, 2019


Michael C. McGarrity
Acting Executive Assistant Director
National Security Branch
Federal Bureau of Investigation
Washington, D.C.

Attorneys for Defendants the Attorney General, *et al.*

| | | |
|-----------------------------------|---|-------------------------|
| |) | |
| TWITTER, INC., |) | Case No. 14-cv-4480-YGR |
| |) | |
| Plaintiff, |) | |
| |) | |
| |) | |
| v. |) | |
| |) | |
| WILLIAM P. BARR, United States |) | |
| Attorney General, <i>et al.</i> , |) | |
| |) | |
| Defendants. |) | |
| |) | [PROPOSED] ORDER |
| |) | |

Twitter, Inc. v. Barr, et al., Case No. 14-cv-4480-YGR
[PROPOSED] ORDER

1 Declaration, or, in the Alternative, Motion to Dismiss in Light of the Attorney General's
2 Assertion of the State Secrets Privilege, and any submissions in support thereof or in
3 opposition thereto, hereby **ORDERS** that the Order to Show Cause is hereby **DISCHARGED**
4 and further **ORDERS** that Plaintiff's request to access the Classified Steinbach Declaration is
5 **DENIED**.

6
7 IT IS SO **ORDERED**, this _____ day of _____, 2019.
8
9

10 Dated: _____
11

12 HON. YVONNE GONZALEZ ROGERS
13 UNITED STATES DISTRICT JUDGE
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

JOSEPH H. HUNT
Assistant Attorney General
DAVID L. ANDERSON
United States Attorney
ANTHONY J. COPPOLINO
Deputy Branch Director
JULIA A. HEIMAN
Senior Counsel
CHRISTOPHER HEALY
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch

P.O. Box 883
Washington, D.C. 20044
Telephone: (202) 616-8480
Facsimile: (202) 616-8470
Email: julia.heiman@usdoj.gov

Attorneys for Defendants the Attorney General, *et al.*

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

| | | |
|-----------------------------------|---|-------------------------|
| _____ |) | |
| TWITTER, INC., |) | Case No. 14-cv-4480-YGR |
| |) | |
| Plaintiff, |) | |
| |) | |
| |) | |
| v. |) | |
| |) | |
| WILLIAM P. BARR, United States |) | |
| Attorney General, <i>et al.</i> , |) | |
| |) | |
| Defendants. |) | |
| _____ |) | [PROPOSED] ORDER |

The Court, having considered the Defendants' Request that the Court Discharge the
Order to Show Cause and Deny Plaintiff's Request for Access to the Classified Steinbach

1 Declaration, or, in the Alternative, Motion to Dismiss in Light of the Attorney General's
2 Assertion of the State Secrets Privilege, and any submissions in support thereof or in
3 opposition thereto, hereby **ORDERS** that the Defendants' motion is **GRANTED**, and
4 **FURTHER ORDERS** that this action is hereby **DISMISSED**.

5
6 IT IS SO **ORDERED**, this _____ day of _____, 2019.

7
8
9 Dated: _____

10 _____
11 HON. YVONNE GONZALEZ ROGERS
12 UNITED STATES DISTRICT JUDGE
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28